巡回符号とCRC

情報数理学特別講義I 第5回

2025-11-05

今回の講義の目標（学ぶこと）

- 巡回符号の定義と多項式表現
- 巡回符号は生成多項式により一意に定義される
    - 生成多項式により巡回符号の次元が決まる.
- 巡回符号の符号化
- 巡回符号の生成行列とパリティ検査行列

巡回符号

誤り訂正符号の実用上重要な線形符号のクラスに巡回符号がある.
講義で今後登場するCRC(Cyclic Redundancy Check)やBCH符号も巡回符号の一種である.

以降では，巡回符号の基本的な性質を述べる.
巡回符号の定義を述べた後，巡回符号が**生成多項式**によって特徴づけられることを示す.
そして巡回符号の生成行列とパリティ検査行列が生成多項式を用いてどのように表されるかを説明する.

巡回符号の定義

$GF(2^q)$ 上の $[n, k]$ 線形符号 $\mathcal{C}$ で，任意の符号語 $\underline{c} = (c_0, c_1, \ldots, c_{n-1})$の巡回シフト $(c_{n-1}, c_0, \ldots, c_{n-2})$も符号語であるとき，符号 $\mathcal{C}$ を **巡回符号(cyclic code)** と呼ぶ.

例えば符号 $\mathcal{C} = \{000, 111\}$ は巡回符号である.

問題１： 長さ4の単一パリティ検査符号は巡回符号であるか？
問題２： 符号 $\mathcal{C} = \{0000, 1000, 0100, 0010, 0001\}$ は巡回符号であるか？

巡回符号の多項式表現

巡回符号は，符号語を $GF(2^q)$ 上の多項式で表すと数学的な取り扱いが容易になる．
すなわち，符号語 $\underline{c} = (c_0, c_1, \ldots, c_{n-1}) \in GF(2^q)^n$ に対応する符号多項式を

$$c(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

によって定める．多項式表現を用いた時，線形符号 $\mathcal{C}$ が巡回符号であるための条件は，
任意の符号多項式 $c(x)$ に対し

$$Rem(xc(x)/(x^n - 1)) \in \mathcal{C}$$

が成り立つことである．ただし，$Rem(xc(x)/(x^n - 1))$ は $xc(x)$ を $x^n - 1$ で割った時の剰余 $(xc(x) \bmod x^n - 1)$ である．

多項式表現による巡回符号の条件

なぜ $Rem(xc(x)/(x^n-1)) \in \mathcal{C}$ の成立が巡回符号の条件かというと

$$\begin{aligned} xc(x) &= c_0x + c_1x^2 + \cdots + c_{n-1}x^n \\ &= c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1} + c_{n-1} \bmod x^n - 1 \end{aligned}$$

から直ちに

$$Rem\left(xc(x)/(x^n-1)\right) = c_{n-1} + c_0x + c_1x^2 + \cdots + c_{n-2}x^{n-1}$$

が得られ，これは巡回符号の定義である $c(x)$ の巡回シフトに一致するからである.
同様に，$c(x)$を i 回巡回シフトさせた

$$Rem\left(x^ic(x)/(x^n-1)\right) = c_{n-i} + c_{n-i+1}x + c_1x^2 + \cdots + c_{n-i-1}x^{n-1} \in \mathcal{C}$$

も成り立つ.

符号多項式と多項式の積もまた符号多項式

一方，$\mathcal{C}$ は線形符号なので，$m(x) = \sum_j m_j x^j, m_j \in GF(2^q)$ とすると，

$$Rem(m(x)c(x)/(x^n-1)) = Rem\left(\sum_j m_j x^j c(x)/(x^n-1)\right)$$
$$= \sum_j m_j Rem\left(x^j c(x)/(x^n-1)\right) \in \mathcal{C}$$

となる．したがって $c(x) \in \mathcal{C}$ ならば任意の$GF(2^q)$上の多項式 $m(x)$ について

$$Rem(m(x)c(x)/(x^n-1)) \in \mathcal{C}$$

が成り立つ．

巡回符号の生成多項式

$GF(2^q)$ 上の $[n, k]$ 巡回符号 $\mathcal{C}$ において，$g(x)$ を符号多項式の中で次数が最小のモニック多項式(最高次の係数が1の多項式)とする（符号多項式 0 は除く）.
このとき，次の性質が成り立つ.

- $g(x)$は一意的に定まる．※つまり，$g(x)$ により巡回符号が定まる.
- $g(x)$ は $\mathcal{C}$ の全ての符号多項式 $c(x)$ を割り切る
- $g(x)$ は $GF(2^q)$ 上の多項式 $x^n - 1$ を割り切る.
- $k = n - \deg g(x)$ ただし $\deg g(x)$ は多項式 $g(x)$ の最大次数を表す.

また，$g(x)$を巡回符号 $\mathcal{C}$ の **生成多項式(generator polynomial)** と呼ぶ.
各性質の証明は 植松 友彦「代数系と符号理論」などを参照ください.

生成多項式の例

例１：長さ3の2元繰り返し符号 $\mathcal{C} = \{000, 111\}$ の生成多項式は,
符号多項式が 0 と $1 + x + x^2$ の
2つなので,

$$g(x) = 1 + x + x^2$$

である．また,

$$x^3 - 1 = (x - 1)(x^2 + x + 1)$$

から，生成多項式 $g(x)$ が $x^3 - 1$ を割りきることがわかる.

練習問題１：長さ4の2元単一パリティ検査符号の生成多項式を求めよ.

練習問題２

長さ4の2元単一パリティ検査符号の符号多項式を生成多項式と多項式の積で書き下してみよ

$0000 \rightarrow$

$1100 \rightarrow$

$1010 \rightarrow$

$1001 \rightarrow$

$0110 \rightarrow$

$0101 \rightarrow$

$0011 \rightarrow$

$1111 \rightarrow$

生成多項式とメッセージ多項式との積の集合は巡回符号

定理：
$GF(2^q)$ 上の多項式 $g(x)$ は $x^n - 1$ を割り切る r 次のモニック多項式とする．このとき，

$$\mathcal{C} = \{m(x)g(x) : m(x) \in GF(2^q)[x], \deg m(x) < n - r\}$$

は生成多項式 $g(x)$ を有する $GF(2^q)$ 上の $[n, k = n - r]$ 巡回符号である．
ただし $GF(2^q)[x]$ は $GF(2^q)$ 上の多項式の集合である．
特に $m(x)$ のことをメッセージ多項式と呼ぶ．

証明

$m(x) \in GF(2^q)[x]$ は $n-r$ 次未満の任意の多項式であることから,
$m(x)g(x) + m'(x)g(x) = m''(x)g(x)$, ただし $m(x) + m'(x) = m''(x)$ となるため, $\mathcal{C}$ は線形符号.
$n-r$ 次未満のメッセージ多項式は異なる符号多項式を与えるので, この線形符号の次元は $k = n - r$. よって以降ではこの線形符号が巡回符号であること($Rem(xc(x)/(x^n-1))$が符号多項式であること)を示す.

※以降, $Rem(xc(x)/(x^n-1))$ を $Rem(xc(x))_{x^n-1}$ と記載する.

$$h(x) = \frac{x^n - 1}{g(x)} = h_0 + h_1 x + \cdots + h_{n-r} x^{n-r}$$

とおくと，$g(x)$はモニック多項式なので $g_r = 1$であり，
$h(x)$ もモニック多項式($h_{n-r} = 1$)となる.
一方，$n - r$ 次未満の多項式 $m(x)$ に対応する符号多項式

$$c(x) = m(x)g(x) = c_0 + c_1 + \cdots + c_{n-1} x^{n-1}$$

に対して，

$$\begin{aligned} Rem(xc(x))_{x^n-1} &= Rem(xc(x) - c_{n-1}\left(x^n - 1\right))_{x^n-1} \\ &= Rem(xm(x)g(x) - c_{n-1}h(x)g(x))_{x^n-1} \\ &= Rem((xm(x) - c_{n-1}h(x))g(x))_{x^n-1} \end{aligned}$$

が成り立つ.

$$Rem(xc(x))_{x^n-1} = Rem((xm(x) - c_{n-1}h(x))g(x))_{x^n-1}$$

ここで，$g(x)$ が r次 のモニック多項式であることから，$c_{n-1} = g_r m_{n-r-1} = m_{n-r-1}$ となる．そして $h(x)$ は $n-r$ 次のモニック多項式であることから，$xc(x)$ の $n-r$ 次の係数と $c_{n-1}h(x)$ の $n-r$次の係数はともに $m(x)$ の $n-r-1$次の係数 m_{n-r-1} に等しい．よって

$$\deg\left(xm(x) - c_{n-1}h(x)\right) < n-r$$

となることから,

$$Rem(xc(x))_{x^n-1} = (xm(x) - c_{n-1}h(x))g(x)$$

とかける．つまり $xc(x)$ も符号多項式となる．このことから $\mathcal{C}$ は巡回符号となる．□

巡回符号の符号化

$g(x)$ を r 次の生成多項式とする符号長 n の巡回符号において,
メッセージ多項式 $m(x)$ の符号化は

$$m(x) \Longrightarrow m(x)g(x)$$

によって行われる．ただし，$m(x)$ の次数は $n-r$ 次未満である.

この符号化は，非組織符号化と呼ばれ，符号多項式にメッセージが表れない.
組織符号化（符号多項式の一部がメッセージになる）をする際には次数を r次上げた
メッセージ多項式に剰余を足し込む

$$m(x) \Longrightarrow x^r m(x) + Rem(m(x))_{g(x)}.$$

証明は略すが，こうして得られた符号多項式の集合も巡回符号となる.

練習問題３（10分）

符号長7の2元巡回符号の生成多項式を$g(x) = 1 + x^2 + x^3$とする.
このとき，次の問いに答えよ.

1. $g(x)$ が $x^7 - 1$ を割り切ることを示せ.
2. メッセージ多項式$1 + x^3$，x，$x + x^2 + x^3$を非組織符号化した際の符号多項式をそれぞれ求めよ.
3. 非組織符号化した際の符号多項式 $x^2 + x^4 + x^5$, $1 + x + x^2 + x^4$, $x^2 + x^3 + x^4 + x^6$ に対応するメッセージ多項式をそれぞれ求めよ.

巡回符号の生成行列とパリティ検査行列

$GF(2^q)$ 上の $[n, k]$ 巡回符号を $\mathcal{C}$ とする．以下では巡回符号 $\mathcal{C}$ の生成行列を求める．
巡回符号 $\mathcal{C}$ は生成多項式

$$g(x) = g_0 + g_1 x + \cdots + x^{n-k}$$

を持ち，$x^j g(x), j = 0, 1, \ldots, k-1$ が線形独立な符号多項式を与える．
これらの符号多項式をベクトルで表すと，

$$\begin{aligned}
g(x) &\leftrightarrow (g_0, g_1, \ldots, g_{n-k-1}, 1, 0, \ldots, 0) \\
xg(x) &\leftrightarrow (0, g_0, g_1, \ldots, g_{n-k-1}, 1, 0, \ldots, 0) \\
x^2 g(x) &\leftrightarrow (0, 0, g_0, g_1, \ldots, g_{n-k-1}, 1, 0, \ldots, 0) \\
&\vdots \\
x^{k-1} g(x) &\leftrightarrow (0, \ldots, 0, g_0, g_1, \ldots, g_{n-k-1}, 1)
\end{aligned}$$

となる．これらのベクトルを行ベクトルとして行列に並べると，

巡回符号 $\mathcal{C}$ の生成行列

$$G = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & 1 & 0 & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k-1} & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & g_0 & \cdots & g_{n-k-2} & g_{n-k-1} & 1 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & & \cdots & \cdots & & \cdots & 1 \end{bmatrix}$$

が得られる.

念のために述べておくと，この生成行列で生成される$[n, k]$巡回符号の次元は k である（G が k 行であることから明らか）.

一方，パリティ検査行列を得るため,

$$g(x)h(x) = x^n - 1$$

に着目する．$k-1$ 次以下の任意の多項式 $m(x)$ に対応する符号多項式は

$$c(x) = m(x)g(x)$$

と書けるので,

$$c(x)h(x) = m(x)g(x)h(x) = m(x)(x^n - 1) = m(x)x^n - m(x)$$

が得られる.
$m(x)$ の次数は $k-1$ 次以下，$m(x)x^n$の次数は n 次以上なので,
$c(x)h(x)$ の次数 $k, k+1, k+2, \ldots, n-1$ の項は全て零である.

すなわち，$j = k, k+1, \ldots, n-1$ の次数の項の係数について

$$c(x)h(x)\text{の } j \text{ 次の係数} = \sum_{i=j-k}^{j} c_i h_{j-i} = 0$$

が成り立つ．これを行列で表すと

$$\begin{bmatrix} h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & 0 & 0 & \ldots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & \ldots & 0 \\ 0 & 0 & h_k & \cdots & h_2 & h_1 & h_0 & \cdots & 0 \\ \vdots & \vdots & & \ddots & & \ddots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & & \cdots & & \cdots & h_0 \end{bmatrix} (c_0, c_1, \ldots, c_{n-1})^T = \underline{0}$$

が得られ，この $n-k$ 行 n 列の行列のランクは $n-k$ なので，

パリティ検査行列は

$$H = \begin{bmatrix} h_k & h_{k-1} & h_{k-2} & \cdots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \cdots & h_1 & h_0 & 0 & \dots & 0 \\ 0 & 0 & h_k & \cdots & h_2 & h_1 & h_0 & \cdots & 0 \\ \vdots & \vdots & & \ddots & & \ddots & & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & & \cdots & & \cdots & h_0 \end{bmatrix}$$

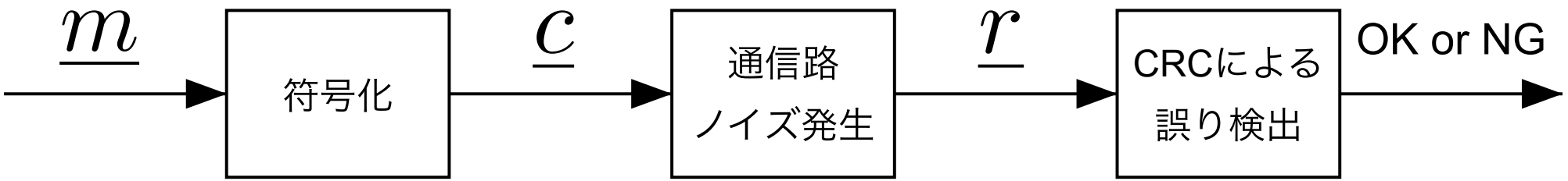
となる．ここで得られたパリティ検査行列 H は,
第1行に $h(x)$ の係数を降べきの順に並べ，さらに残りの $n-k-1$ 個の行に
第1行の巡回シフトを順に並べたものになっている.

練習問題４

生成多項式 $g(x) = 1 + x^2 + x^3$ を持つ 2元 [7,4] 巡回符号について，次の問いに答えよ

1. 生成行列 G を求めよ.
2. パリティ検査行列 H を求めよ.
3. メッセージ $(1, 0, 0, 1)$ を生成行列 G で符号化し，符号語 $\underline{c}$ を求めよ.
4. 上記問いで得られた符号語 $\underline{c}$ をパリティ検査行列 H で検査し，シンドロームが 0 となることを確認せよ.

Cyclic Redundancy Check (CRC)



データの信頼性を確保するため，データの誤り検出に使用される誤り検出手法
通信やデータストレージにおいて，誤り訂正符号と同様，広く使用されている技術.

符号化：生成多項式を用いた剰余による組織符号化
誤り検出：生成多項式の剰余による誤り検出

CRCの符号化と誤り検出方法

パリティサイズが r ビットのCRC符号化をする際には，次数が r 次の生成多項式 $g(x)$ を用い，符号化対象のメッセージ多項式 $m(x)$ に対して $Rem(x^r m(x))_{g(x)}$ を計算.
符号語多項式 $c(x)$ は以下のようになる.

$$c(x) = x^r m(x) + Rem(x^r m(x))_{g(x)}$$

メッセージ $m(x)$ は x^r によって r 次以上の多項式となっており,
$Rem(x^r m(x))_{g(x)}$ は $r-1$次以下の多項式になることから,
$Rem(x^r m(x))_{g(x)}$ が r ビットのパリティビットとして付加されることに相当する.

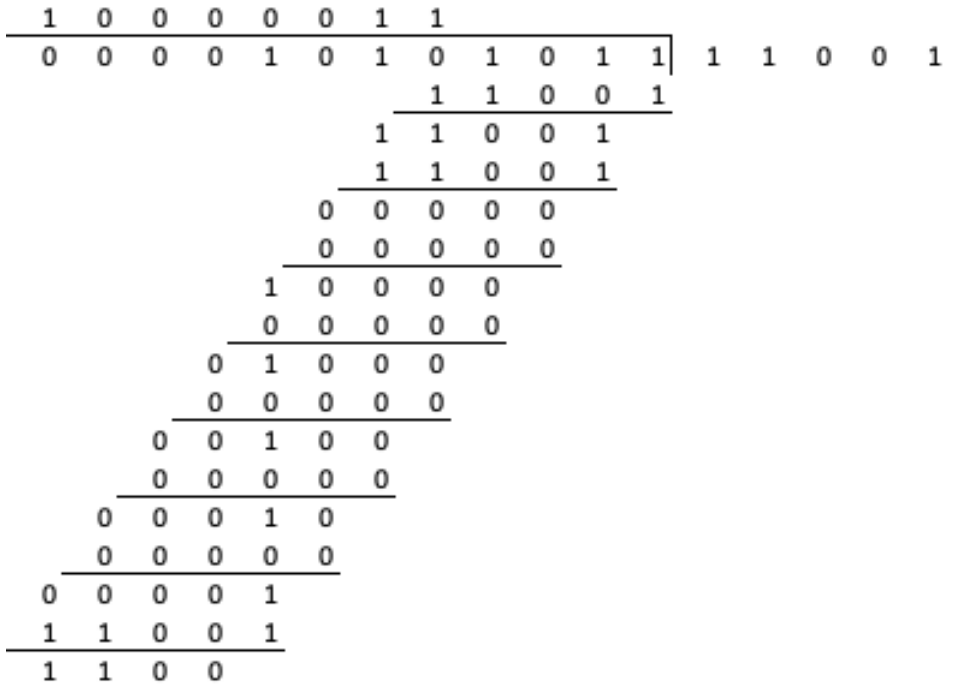
受信側では，受信した受信多項式 $r(x)$ に対して $Rem(r(x))_{g(x)}$ を計算し,
その結果がゼロであれば誤りがないことを確認できる.

多項式の剰余を計算してみよう

$f(x) = 1 + x^2 + x^4 + x^6 + x^7, g(x) = 1 + x + x^4$ のとき,
$Rem(x^4 f(x))_{g(x)}$ を計算してみよう.

$\underline{f} = 10101011$

$\underline{g} = 11001$

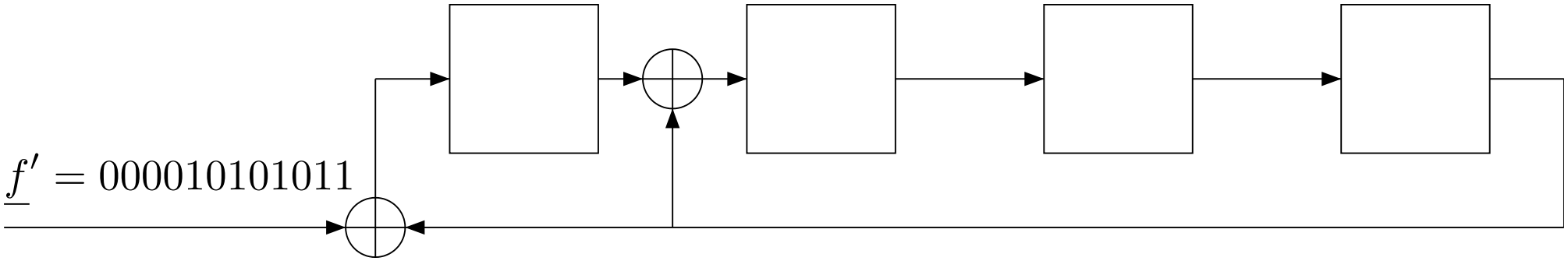


2元ベクトルにして筆算をすると, $Rem(x^4 f(x))_{g(x)} = 1 + x$ が求まる.

この筆算の処理, どこかで見ていませんか？

LFSRは剰余回路

レジスタの初期値を 0000 とした $\underline{g} = 11001$ で結線したLFSRに対して,
$\underline{f'} = 000010101011$ を入力完了したときのレジスタの値が
$Rem(x^4 f(x))_{g(x)}$ となる.



Juliaで確認

```
function lfsr(reg, input)
    rr = (reg << 1) ⊻ input
    if rr >= 16
        rr ⊻= 0b10011
    end
    return rr
end
f = [1,1,0,1,0,1,0,1,0,0,0,0] # x^4(x^7+x^6+x^4+x^2+1)
reg = 0
for fin in f
    global reg = lfsr(reg, fin)
    println(de2bi(reg, width=4)) # 4bitバイナリ出力
end
```

Juliaの実行結果

```
[1, 0, 0, 0]
[1, 1, 0, 0]
[0, 1, 1, 0]
[1, 0, 1, 1]
[1, 0, 0, 1]
[0, 0, 0, 0]
[0, 0, 0, 0]
[1, 0, 0, 0]
[0, 1, 0, 0]
[0, 0, 1, 0]
[0, 0, 0, 1]
[1, 1, 0, 0] # 入力完了時のレジスタの中身
```

LFSRにより $Rem(x^4 f(x))_{g(x)} = 1 + x$ が求まる.

符号多項式の剰余を計算

```
c = [1,1,0,1,0,1,0,1,0,0,1,1] # x^4(x^7+x^6+x^4+x^2+1) + x + 1
reg = 0
for cin in c
    global reg = lfsr(reg, cin)
    println(de2bi(reg, width=4)) # 4bitバイナリ出力
end
[1, 0, 0, 0]
[1, 1, 0, 0]
[0, 1, 1, 0]
[1, 0, 1, 1]
[1, 0, 0, 1]
[0, 0, 0, 0]
[0, 0, 0, 0]
[1, 0, 0, 0]
[0, 1, 0, 0]
[0, 0, 1, 0]
[1, 0, 0, 1]
[0, 0, 0, 0] # レジスタが0 つまり剰余が0
```

符号多項式の剰余を計算(エラーあり)

```
c = [1,1,0,1,0,1,0,1,0,0,1,0] # x^4(x^7+x^6+x^4+x^2+1) + x
reg = 0
for cin in c
    global reg = lfsr(reg, cin)
    println(de2bi(reg, width=4)) # 4bitバイナリ出力
end
[1, 0, 0, 0]
[1, 1, 0, 0]
[0, 1, 1, 0]
[1, 0, 1, 1]
[1, 0, 0, 1]
[0, 0, 0, 0]
[0, 0, 0, 0]
[1, 0, 0, 0]
[0, 1, 0, 0]
[0, 0, 1, 0]
[1, 0, 0, 1]
[1, 0, 0, 0] # レジスタが非ゼロ、つまり誤りを検出.
```